UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,651	01/28/2002	Steven M. Blumenau	10830.0033.DVUS01	5520

27927 7590 12/23/2004

RICHARD AUCHTERLONIE
NOVAK DRUCE LLP
1615 L ST NW
SUITE 850
WASHINGTON, DC 20036

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 12/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,651	BLUMENAU ET AL.	
	Examiner	Art Unit	
	Kyung H Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the Appplication filed 1/28/2002.
2. **Claim 7** is amended, **claims 10 – 12** are added, **claims 1 - 12** are pending on this application. **Claims 1, 7, 12** are independent claims.

Response to Arguments

3. Applicant's arguments filed 7/28/2004 have been fully considered but they are not persuasive. The applicant have argued the following:

3.1. Applicant Remarks states that the referenced prior art, Best (4,465,901), Little (5,998,858) and Rigal (5,881,155), does not disclose: (1) one input and one output for a chip used to process data, (2) both encryption and decryption procedures are performed, and (3) the Best prior art does not disclose an encryption program.

Examiner respectfully states that Best discloses one input (see Best col. 6, lines 48-53), one output (see Best col. 7, lines 45-47), an encryption program for encryption/decryption procedures (see Best col. 4, lines 41-43; col.7, lines 49-53), and the capability to both encrypt and decrypt data (see Best col. 7, lines 49-53).

The disclosure of these limitations by the referenced prior art forms the basis for the rejection of claims 1, 3 - 7, 9, 12 due to U.S.C. 103(a) based on the referenced prior art.

3. 2. Applicant Remarks state that the referenced prior art does not disclose the three limitations stated in Claims 10, 11 and 12. The three limitations are: (a) a monolithic semiconductor circuit chip, (b) an electrically erasable and programmable read-only memory, and (c) a metal shielding layer over memory. Examiner respectfully states that these three limitations are disclosed by the combination of the three referenced prior arts, Best, Little, and Rigal.

Best in view of Little discloses an integrated circuit chip that is: (a) a monolithic semiconductor circuit chip (see Little col. 5, lines 2-5) and (b) electrically erasable and has a programmable read-only memory (see Little col. 7, line 66 - col. 8, line 6; col. 6, lines 6-19). Best in view of Rigal discloses a metal shielding layer over memory (see Rigal col. 6, lines 32-34) The guard ring in Rigal is stated to be a metallic layer that protects the entire chip (including its memory).

The disclosure of the three limitations by the referenced prior art forms the basis for the rejection of claims 10, 11, 12 due to U.S.C. 103(a) based on referenced prior art.

3. 3. Rigal discloses a semiconductor chip operating as a security device to

prevent unauthorized access to stored information. Little discloses an integrated circuit chip with a combination of security mechanisms to protect stored information. These features are obvious and necessary features for any integrated chip operating in an IT environment due to the strengthened security for data protection. The combination of Best and Rigal and the combination of Best and Little would be an obvious combination to obtained chip with strengthened security.

Examiner has re-examined the application and Applicant Remarks. The re-examination and analysis of Applicant Remarks are not persuasive. Therefore, the rejection of claims 1-12 is proper and maintained herein.

Claim Rejections - 35 USC § 103

4. **Claims 1, 3 –7, 9, 12,** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Best,** (U.S. Patent No. 4,465,901) in view of **Rigal** (U.S. Patent No. 5,881,155).

Regarding claims 1, 7, Best discloses the art of cryptographic microprocessor authentication protocol, which resides in an electronic circuit chip (see Fig.1) comprising:

a) a memory for storing information defining an encryption procedure assigned to *the electronic circuit chip* (see col. 4, lines 47-52, and col. 4, lines 57-60)

b) at least one input to *the electronic circuit chip* for writing, to the memory, the information defining the encryption procedure assigned to *the electronic circuit chip,* and for receiving data to be encrypted by the encryption procedure assigned to *the electronic circuit chip* (see col. 4, lines 41-56)

c) encryption circuitry for reading from the memory the information defining the encryption procedure assigned to *the electronic circuit chip*, and for encrypting the data from said at least one input to *the electronic circuit chip* according to the encryption procedure assigned to *the electronic circuit chip*, to produce encrypted data (see col. 6, lines 19-21 and col. 7, line 60 - col. 8, line 4);

d) at least one output from *the electronic circuit chip* for transmitting the encrypted data produced by the encryption circuitry (see col. 7, lines 45-47);

e) wherein the electronic circuit chip is constructed so that the information defining the encryption procedure assigned to the electronic circuit chip cannot be read from the memory from any output of the electronic circuit chip (see col. 5, lines 56-60, and col. 13, lines 14-29)

f) wherein the electronic circuit chip is constructed so that it is virtually impossible to recover the information in the memory by probing, inspection, or disassembly (see col. 16, lines 42-50: *"If the enciphered program is small enough it may be stored in ROM in cipher or transposed form on the crypto-microprocessor chip to prevent a pirate from reading the program from a photographic enlargement of the chip or by probing an easily found internal bus....."*, and col. 18, lines 26-37)

g) **Best** discloses metal, oxide and semiconductor (MOS) but does not specifically mention a metal shielding layer over the memory. However, **Rigal** in analogous art discloses a metal shielding layer (see FIGS. 5 and 6, and col. 6, lines 30-37: *"....Guard ring 50 is a metallic layer used to electrically isolate the protected chip from external electrical influences. Its specific dimensions are not of particular importance. For example, guard ring 50 can be formed at the periphery of the protected chip 10 and on a surface of the protective chip 20..")* It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Best** with a metallic layer over EEPROM as taught in **Rigal.** One would have been motivated to substitute the metallic layer in **Rigal** in order to reduce tempering capability, so that the information stored in the memory cannot be read by visual inspection or probing and the information can also be resistant to interference, which enhances protection of the confidential information stored in the chip.

Regarding claims 3 and 9, Best discloses the electronic circuit chip, wherein the memory is an electrically erasable and programmable read-only memory (see col. 14, lines 3-7: *"If the S-boxes are electrically alterable read-only memory then a battery is not needed and loading circuit 76 would be changed accordingly."* and col. 20, lines 46-61).

Regarding claim 4, **Best** discloses the electronic circuit chip, wherein said encryption circuitry includes a microprocessor for computing the encrypted data (see col. 18, line 66- col. 19, line 12).

Regarding claim 5, **Best** discloses the electronic circuit chip as claimed in claim 4, wherein the microprocessor is constructed to execute an encryption program stored in the memory, and the encryption program defines the encryption procedure assigned to the electronic circuit chip (see col. 19, lines 36-57).

Regarding claim 6, **Best** discloses the electronic circuit chip as claimed in claim 4, wherein said microprocessor is programmed to read an encryption key from the memory, and to compute the encrypted data using the encryption key, and the encryption key defines the encryption procedure assigned to the electronic circuit chip (see col. 5, line 63- col. 6, line 12).

Regarding Claim 12 (NEW), **Best** discloses an electronic circuit chip comprising:

a) - g) These limitations encompass the same scope of the invention as that of the claim 1. a - g, therefore these limitations are rejected for the same reason as the claim 1. a - g.

h) Rigal in analogous art discloses the electronic circuit chip is a semiconductor integrated circuit chip, the memory is an electrically erasable and programmable read-only memory (*EEPROM*) , and the *metal* shielding layer over the memory is an upper layer of metal on the electronic circuit chip; (see **Rigal,** col. 4, lines 53-62, *".....provided with an electrically erasable memory (EEPROM or flash EPROM), a*

volatile memory (RAM) and encryption capabilities." and **Rigal,** FIGS. 5 and 6, and col. 6, lines 30-37: *"....Guard ring 50 is a metallic layer used to electrically isolate the protected chip...)* It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Best's** *semiconductor chip,* with the metal shielding layer over the EEPROM as taught in **Rigal.** One would have been motivated to substitute the *type of* chip as **Rigal** in order to make a reliable and efficacious solution for enhanced security against an unlawful attempt to gain access to data stored in a security device.

i) wherein *the microprocessor* is programmed to read an encryption key from the memory, and to compute the encrypted data using the encryption key, and the encryption key defines the encryption procedure assigned to the electronic circuit chip. (see **Best,** col. 6, lines 48-55, and col. 9, lines 54-57: *"Crypto-microprocessors which use this encryption method are shown in FIGS. 1, 8, 9, and 15. To decipher a byte the enciphered byte is exclusive-ORed with a scrambled function of the byte's address.")*

5. **Claims 2, 8, and 10, 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Best- Rigal** as applied to claims 1, 7 above and further in view of **Little et al.** (U.S. Patent No. 5,998,858).

Regarding claims 2, 8, Best discloses the electronic circuit chip with a type of semiconductor integrated circuit chip (see col. 18, line 66- col. 19, line 12), however, Best's chip is not *monolithic* semiconductor integrated circuit chip. **LIttle** discloses a *monolithic semiconductor chip* (see col. 18, lines 26-37: *"The electronic data module 100, ... is designed to hermetically house a monolithic semiconductor chip 135 that may comprise a host of circuit elements such as memory, microprocessors, multiplexing circuitry and electrostatic discharge protection circuitry.")* It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Best** with a *monolithic semiconductor chip* as taught in **LIttle.** One would have been motivated to substitute the *monolithic semiconductor* chip in **LIttle** in order to enhance detection associated with an unlawful attempt to gain access data stored in the chip.

Regarding claims 10, 11 (NEW), **Best** discloses the electronic circuit chip as claimed in claims **1, 7**, wherein the electronic circuit chip is a monolithic semiconductor integrated circuit chip, (see **Little**, col. 18, lines 26-37) the memory is an electrically erasable and programmable read-only memory, (see **Best**, col. 14, lines 3-7, and **Rigal,** col. 4, lines 53-62) and the metal shielding layer over the memory is an upper layer of metal (see **Rigal**, col. 6, lines 30-37) on the electronic circuit chip. (see Best, col. 16, lines 42-46) It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Best** with a metallic layer over EEPROM as taught in **Rigal** and monolithic semiconductor chip as taught in **Little**. One would have been motivated to combine the metallic layer

in **Rigal** and monolithic chip in **Little** in order to make an effective chip for reducing tampering capability, so that the information stored in the memory cannot be read by visual inspection or probing, which enhances protection of the confidential information stored in the chip.

Conclusion

6. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
Dec. 12, 2004

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100